The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
8/10/2010

SUBJECT:
Vulnerability in Microsoft Office Excel Could Allow Remote Code Execution (MS10-057)

OVERVIEW:
A vulnerability has been discovered in Microsoft Office Excel, a spreadsheet application. This vulnerability could allow remote code execution if a user opens a specially crafted Excel file. The file may be received as an email attachment, or downloaded via the web. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

Microsoft Office XP
Microsoft Office 2003
Microsoft Office 2004 for Mac
Microsoft Office 2008 for Mac
Open XML File Format Converter for Mac

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been identified in Microsoft Office Excel that could allow an attacker to take complete control of an affected system. This vulnerability exists because of the way Microsoft Office Excel parses the Excel file format when processing Excel files (.xls). This can be triggered by opening a specially crafted Excel file and can be exploited via email or through the web. In an email based scenario, the user would have to open the specially crafted Excel file as an email attachment. In a web based scenario, a user would have to open the specially crafted Excel file that is hosted on a website. When the user opens the Excel file, the attacker's supplied code will execute.

Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Consider using the Microsoft Office Isolated Conversion Environment (MOICE - http://support.microsoft.com/kb/935865).

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/bulletin/ms10-057.mspx
http://support.microsoft.com/kb/935865

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2562

Security Focus:
http://www.securityfocus.com/bid/42199